APPENDIX OF CLAIMS

The text of the claims involved in the appeal reads:

1. Method for controlling access to protected contents on a server, the method requiring the following components to be present:

a) a server

b) a client

c) a reader for a mobile security module

d) a security module having at least one protected area for storing a key

e) a data line for communications between client and server

characterized by the following steps:

aa) sending to the server of a request to call up protected-access contents

bb) sending from the server to the client of an authentication module to be run in the client

cc) execution of an authentication protocol for authenticating the mobile security module and, where appropriate, its holder by means of the authentication module

dd) if the authentication in step cc) was successful, addition to the request in step aa) of a session ID which was generated in the course of the communications between the authentication module and the server

ee) sending of the new request to the server application

ff) checking of the session ID in the request to see that it is recorded in the server

gg) processing of the content requested for transmission and searching of the contents for further links to other protected-access contents

hh) addition of the session ID to the links identified

ii) sending of the content modified as in step hh) to the client.

2. Method according to claim 1, characterized in that the server is a web server and the protected contents are web pages which are called up via a browser by a URL request from a client.

3. Method according to claim 1, characterized in that the authentication protocol is executed in the followed steps:

jj) generation of a random number by the server application when the content requested is access-protected and the requirements for access have not been satisfied, and sending of the random number to the authentication module

kk) sending of the random number from the authentication module to the mobile security module

ll) generation in the mobile security module of a digital signature which takes account of the identity number of the mobile security module, the random number and the key of the mobile security module

mm) sending of the digital signature to the server

nn) checking of the correctness of the digital signature using the security module of the server.

4. Method according to claim 2, characterized in that the server application is a servlet and the client authentication module is an authentication applet and in that on receipt of a URL

request the servlet checks the URL request for the presence of a session ID and if there is no session ID present sends an authentication applet containing a random number to the client.

5. Method according to claim 1, characterized in that the communications between client and server take place via SSL (secure sockets layer) as the transmission protocol.

7. Method according to claim 3, characterized in that the digital signature is generated by means of a symmetrical encryption algorithm with the help of a secret key agreed between client and server, or by means of an asymmetrical encryption algorithm with the help of a private key, the server being in possession of the public key.

8. Method according to claim 7, characterized in that the symmetrical encryption algorithm is DES or triple DES and the asymmetrical encryption algorithm is RSA, DSA or an elliptic curve algorithm.

9. Method according to claim 4, characterized in that if the digital signature does not agree, the servlet sends an error message to the client applet.

12. Method according to claim 1, characterized in that the session ID is given a period of validity.

13. Method according to claim 12, characterized in that the session ID loses its validity on expiry of a fixed time or when a session is terminated by means of a log-off page.

14. Method according to claim 1, characterized in that the session ID generated in step dd) is recorded in a table and in that the presence of an entry in the table is a requirement for access to all the protected-access pages.

23. A method, in a client, for controlling access to protected contents, the method comprising:

sending a request for protected content to a server;

receiving an authentication applet and a random number from the server, wherein the random number is generated at the server;

executing the authentication applet;

sending, by the authentication applet, the random number to a mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number;

receiving, by the authentication applet, the cryptographic signature from the mobile security module;

sending, by the authentication applet, the cryptographic signature to the server; and

responsive to the server authenticating the cryptographic signature, receiving a session identifier from the server.

24. The method of claim 23, further comprising:

sending a second request for the protected content to the server, wherein the second request includes the session identifier.

25. The method of claim 23, wherein the mobile security module includes an individual number for the mobile security module and wherein the mobile security module generates the cryptographic signature based on the individual number.

26. The method of claim 25, further comprising:

receiving, by the authentication applet, the individual number from the mobile security module; and

sending, by the authentication applet, the individual number to the server for authentication.

27. An apparatus, in a client, for controlling access to protected contents, the apparatus comprising:

means for sending a request for protected content to a server;

means for receiving an authentication applet and a random number from the server, wherein the random number is generated at the server;

means for executing the authentication applet;

means for sending, by the authentication applet, the random number to a mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number;

means for receiving, by the authentication applet, the cryptographic signature from the mobile security module;

means for sending, by the authentication applet, the cryptographic signature to the server;

and

means for responsive to the server authenticating the cryptographic signature, receiving a session identifier from the server.

28. The apparatus of claim 27, further comprising:

means for sending a second request for the protected content to the server, wherein the second request includes the session identifier.

29. The apparatus of claim 27, wherein the mobile security module includes an individual number for the mobile security module and wherein the mobile security module generates the cryptographic signature based on the individual number.

30. The apparatus of claim 29, further comprising:

means for receiving, by the authentication applet, the individual number from the mobile security module; and

means for sending, by the authentication applet, the individual number to the server for authentication.

31. The apparatus of claim 27, wherein the mobile security module is a chip card and wherein the client includes a chip card reader.

32. The apparatus of claim 27, wherein the client is a Web client, wherein the server is a Web server, and wherein the protected content is a Web page.

33. A computer program product, in a computer readable medium, for controlling access to protected contents, the computer program product comprising:

instructions for sending a request for protected content to a server;

instructions for receiving an authentication applet and a random number from the server, wherein the random number is generated at the server;

instructions for executing the authentication applet, wherein the applet is configured to perform the following steps:

send the random number to a mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number;

receive the cryptographic signature from the mobile security module;

send the cryptographic signature to the server; and

responsive to the server authenticating the cryptographic signature, receive a session identifier from the server.

EVIDENCE APPENDIX

There is no additional evidence to be reviewed on appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.